UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/726,433	12/01/2000	Toshio Kuroiwa	0102/0149	1408

21395 7590 08/30/2004

LOUIS WOO
LAW OFFICE OF LOUIS WOO
717 NORTH FAYETTE STREET
ALEXANDRIA, VA 22314

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 08/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/726,433	**Applicant(s)** KUROIWA ET AL.	
	Examiner Samson B Lemma	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on *01 December 2000*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *02/06/2001*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims **1-22** have been examined.

Priority

2. Receipt is acknowledged of papers submitted under 35 U.S.C. 119 (a)-(d), which papers have been placed of record in the file.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 1, 3, 5, 8, 10, 12,15, 16, 19 and 20** are rejected under 35 U.S.C. 103(a) as being unpatentable over Eyer et al. (hereinafter referred to as Eyer)(U.S. Patent No. 5,485,577) in view of Funakoshi et al. (hereinafter referred to as Funakoshi) (U.S. Patent No. 6,401,207)

5. **As per claim 1, 3, 5, 8, 10 and 12 , Eyer** discloses a method/apparatus/transmission medium for/of transmitting contents information, comprising the steps of:

- Generating a first-key signal representative of a first key from first-key base information being a base of the first key; (figure 2, ref. Num 50, figure 2, ref. Num 42)
  (first- key is interpreted by the office to be "Working keys" and is generated by the "working key generator" and the first-key base information is interpreted by the office as the "program pre-key", generating a working key from the program pre-key information meets the recitation of this limitation.)

- Encrypting contents information into encryption-resultant contents information in response to the first-key signal; (figure 1, ref. Num 10; column 4, lines 33-35);
  (It is interpreted by the office that the Encryption-resultant contents as " Encrypted Data In " and is encrypted by the working key or the first key or the first-key signal from the Data or the contents. In other words the content or the DATA is encrypted by the first-key signal or Working key and becomes the

encryption-resultant contents or “Encrypted Date IN” as shown in the figure 1, ref. Num 10)

- Generating a second-key signal representative of a second key (figure 2, ref. Num 34)
(the second key signal is interpreted by the office to be Category Key representative of the second key or Category Key) (column 4, lines 61-63)

- Encrypting the first-key base information into encryption resultant first-key base information in response to the second-key signal; (figure 2, ref. Num 42, 34, 44) (it is interpreted by the office that the first-key base information as Program Pre-Key and resultant first-key base information as Encrypted Program Pre-Key and is derived in response to the second-key signal or the Category Key.)

- Transmitting the encryption-resultant contents information (figure 1, ref. Num 10)
the encryption-resultant first-key base information, (figure 2, ref. Num 44) (The encryption-resultant contents information is interpreted by the office to be the Encrypted Program pre-key as explained above)

Eyer does not explicitly discloses generating a second-key signal representative of a second key on the basis of initial-value information of a given initial value according to a predetermined key generation algorithm and transmitting the initial value information and algorithm identification information for identifying the predetermined key generation algorithm.

However, In the same field of endeavor, Funakoshi discloses how, an authentication key which is interpreted to be the second key by the office, can be generated on the first unit on the basis of initial-value or the seed generated at the first unit according to a predetermined key generation algorithm and transmitting the initial-value information or the seed to the second- unit and this second unit receives the seed through its seed receiving portion and by identifying the predetermined key generation algorithm, the second unit generates a key form the initial-value information or the seed by encoding this initial value or seed which has been received from the first-unit and eventually producing the same key which is the same as the authentication key which had been generated at the first unit. (column 2, lines 59-67; column 3, lines 1-22). Accordingly, It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the key generation and transmitting technique and method as per teachings of Funakoshi into the method of transmitting contents information as taught by Eyer in order to discourage unauthorized users to easily identify or crack the key which has been used to encrypt the contents as well as securely protecting both the transmitting and recording of contents from illegal users.

6. **As per claims 15,16,19 and 20** **Eyer** discloses a method/apparatus/ for or of decrypting encryption-resultant contents information generated by an encrypting side which implements the
steps of

- Generating a first-key signal representative of a first key from first-key base information being a base of the first key; (figure 2, ref. Num 50, figure 2, ref. Num 42)

(first- key is interpreted by the office to be "Working keys" and is generated by the "working key generator" and the first-key base information is interpreted by the office as the "program pre-key", generating a working key from the program pre-key information meets the recitation of this limitation.)

- Encrypting contents information into encryption-resultant contents information in response to the first-key signal; (figure 1, ref. Num 10; column 4, lines 33-35);

(the content or the DATA is encrypted by the first-key signal or Working key and becomes the encryption-resultant contents or "Encrypted Date IN" as shown in the figure 1, ref. Num 10)

- Generating a second-key signal representative of a second key (figure 2, ref. Num 34)

(the second key signal is interpreted by the office to be Category Key signal representative of the second key or Category Key) (column 4, lines 61-63)

- Encrypting the first-key base information into encryption resultant first-key base information in response to the second-key signal; (figure 2, ref. Num 42, 34, 44) (it is interpreted by the office that the first-key base information as Program Pre-Key and resultant first-key base information as Encrypted Program Pre-Key and is derived in response to the second-key signal or the Category Key.)

- Identifying the predetermined key generation algorithm in response to algorithm identification information for identifying the predetermined key generation algorithm; (figure 2B, ref 232)

- Generating a second.-key signal representative of a second key. (figure 3, ref. Num 58)

- Decrypting encryption-resultant first-key base information into original first-key base information in response to the second-key signal; (figure 3, ref. Num 68) (As it has been explained above the second-key signal is interpreted by the office as the Category-key and the encryption-resultant first-key base information is interpreted as the Encrypted Program Pre-key information, the decryption is done as shown at figure 3, ref. Num 68 and the result is the original first-key base information or the Program Pre-key)

- Generating a first-key signal representative of a first key from the original first-key base information; and (figure 3, ref. Num 74) (As It has been explained in previous limitation the first-key base information or the Program Pre-key is first goes through the one-way function and the first key or the working key is generated from the first-key base information or the program pre-key by the working key generator as shown in figure 3, ref. Num 74).

- Decrypting encryption-resultant. contents information into original contents information in response to the first-key signal.(figure 1,ref. Num 20)

(As explained previously, the encryption-resultant contents information is interpreted as the Encrypted Date In as shown in figure 1, ref. Num 10 and decrypted by the first-key signal or the working key as shown in figure 1, ref. Num 20 and the original contents information or the decrypted data out will be derived.)

Eyer does not explicitly discloses

Identifying the predetermined key generation algorithm in response to algorithm identification information for identifying the predetermined key generation algorithm and generating a second-key signal representative of a second key on the basis of initial-value information and the identified key generation algorithm;

However, In the same field of endeavor, Funakoshi discloses how, the receiver side or the second unit identifies the predetermined key generation algorithm and generate an authentication key which is interpreted by the office to be the second key on the basis of initial-value information or the seed received from the first unit. In other words an authentication key or the second key, is generated on the receiver side or the second unit on the basis of initial-value information or seed received from the first unit and the identified key generation algorithm found from the information sent by the first unit. (column 2, lines 59-67; column 3, lines 1-22).

Accordingly, It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the key generation and transmitting technique and method as per teachings of Funakoshi into the method of decrypting contents information as taught by Eyer in order to discourage unauthorized users to easily identify or crack the encryption or decryption key which has been used to encrypt/decrypt the contents as well as securely protecting both the transmitting and recording of contents from illegal users.

7. **Claims 2, 4, 6, 9, 11 and 13** are rejected under 35 U.S.C. 103(a) as being unpatentable over Eyer et al. (hereinafter referred to as Eyer)(U.S. Patent No.

5,485,577) in view of Funakoshi et al. (hereinafter referred to as Funakoshi) (U.S. Patent No. 6,401,207) and further in view of Iisuka et al. (hereinafter referred to as Iitsuka) (U.S. Patent No. 6,463,151)

8. **As per claims 2, 4, 6, 9, 11 and 13** **Eyer** discloses the method/apparatus/ transmission medium for /of recording contents information, comprising the steps of:

- Generating a first-key signal representative of a first key from first-key base information being a base of the first key; (figure 2, ref. Num 50) (first- key is interpreted by the office to be "Working keys" and is generated by the working key generator)
- Encrypting contents information into encryption-resultant contents information in response to the first-key signal; (figure 1, ref. Num 10; column 4, lines 33-35);
  (the content or the DATA is encrypted by the first-key signal or Working key and becomes the encryption-resultant contents or "Encrypted Date IN" as shown in the figure 1, ref. Num 10)

- Generating a second-key signal representative of a second key (figure 2, ref. Num 34)
  (the second key signal is interpreted by the office to be Category Key signal representative of the second key or Category-Key) (column 4, lines 61-63)

- Encrypting the first-key base information into encryption resultant first-key base information in response to the second-key signal; (figure 2, ref. Num 42, 34, 44) (it is interpreted by the office that the first-key base information as Program Pre-Key and resultant first-key base information as Encrypted Program Pre-Key and is derived in response to the second-key signal or the Category Key.)

Furthermore Eyer discloses transmitting the encryption-resultant contents information (figure 1, ref. Num 10)

- Eyer further discloses Transmitting the encryption-resultant contents information (figure 1, ref. Num 10), Eyer also teaches transmitting the encryption-resultant first-key base information, (figure 2, ref. Num 44) (The encryption-resultant contents information is interpreted by the office to be the Encrypted Program pre-key as explained above)

Eyer does not explicitly discloses generating a second-key signal representative of a second key on the basis of initial-value information of a given initial value according to a predetermined key generation algorithm and transmitting the initial value information and algorithm identification information for identifying the predetermined key generation algorithm.

However, In the same field of endeavor, Funakoshi discloses how, an authentication key which is interpreted to be the second key by the office, can be generated on the first unit on the basis of initial-value or the seed generated at the first unit according to a predetermined key generation algorithm and transmitting the initial-value information or the seed to the second- unit and this second unit receives the seed through its seed receiving portion and by identifying the predetermined key generation algorithm, the second unit generates a key form the initial-value information or the seed by encoding this initial value or seed by the predetermined key generation algorithm. (column 2, lines 59-67; column 3, lines 1-22).

Accordingly, It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the key generation and transmitting technique and method as per teachings of Funakoshi into the method of transmitting contents information as taught by Eyer in order to discourage unauthorized users to easily identify or crack the key which has been used to encrypt the contents as well as securely protecting both the transmitting and recording of contents from illegal users.

The combination of Eyer and Funakoshi does not explicitly discloses recording the encryption-resultant contents information recording the encryption-resultant first-key base information, the initial-value information, and algorithm identification information for identifying the predetermined key generation algorithm.

However, in the same field of endavour, Iitsuka

discloses the recording of content and other information on the recording medium, (column 3, lines 16-21; column 7, lines 10-16).

Accordingly, It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to add the features of recording content and other information on the recording medium as per teachings of Iitsuka into the transmitting method taught by the combination of Eyer and Funakoshi, in order to discourage illegal recording of contents by unauthorized users as well as securely protecting both the transmitting and recording of contents.

9. **Claims 7, 14, 17, 18, 21 and 22** are rejected under 35 U.S.C. 103(a) as being unpatentable over Eyer (U.S. Patent No. 5,485,577) in view of Funakoshi (U.S. Patent No. 6,401,207) and further in view of Jansen et al. (hereinafter referred to as Jansen) (U.S. Patent No. 6,587,562)

10. **As per claims 7 and 14,** the combination of Eyer and Funakoshi discloses the method/apparatus of generating a key as applied to claim 3 and 10 above. Furthermore Funakoshi discloses a method/ apparatus of generating a second-key signal representative of a second key on the basis of initial-value information of a given initial value according to a predetermined key generation algorithm; (column 2, lines 59-67; column 3, lines 1-22).(the interpretation is explained in the previous claims)

The combination of Eyer and Funakoshi does not explicitly teach the means for generating the second-key signal comprises a linear feedback shift register using a specified irreducible primitive polynomial.

However, in the same field of endeavor, **Jansen** discloses the method of generating the stream of data items (key) signal comprises a linear feedback shift register using the primitive polynomial. (column 6, lines 20-35; column 6, 47-58; column 5, lines 51-54; column 5, lines 65-67).

Accordingly, It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the signal generating method by using a linear feedback shift register as per teachings of Jasen into the key generation method as taught by the combination of Eyer and Funakoshi, for purpose of providing a synchronous data-stream generator which is more resistance against known attacks and providing improved data-stream generator that is suitable for use in digital consumer electronics systems offering a speed suitable for encryption/decryption of digital audio/video signals.

11. **As per claims 17 and 21**, the combination Eyer, Funakoshi and Jansen discloses an apparatus as applied to claims 16 and 20 above. Furthermore, Funakoshi discloses an apparatus, wherein the identifying means comprises means for selecting one from among a plurality of key generation algorithms in response to the algorithm

identification information as the identified key generation algorithm.(column 2, lines 59-67; column 3, lines 1-22)

12. **As per claims 18 and 22**, the combination of Eyer, Funakoshi and Jansen discloses an apparatus as applied to claims 17 and 21 above.

Furthermore, Jason discloses an apparatus, wherein the means for generating the second-key signal comprises a linear feedback shift register having a feedback object position which is set in accordance with a primitive polynomial in the identified key generation algorithm. (column 6, lines 20-35; column 6, 47-58; column 5, lines 51-54; column 5, lines 65-67).

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.(See PTO-Form 892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 703-305-8745. The examiner can normally be reached on Monday-Fridary (8:00 am---4:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

08/26/2004

Gilberto

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100